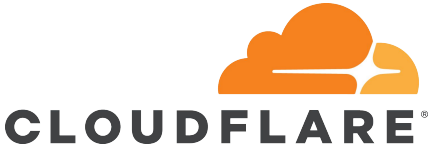


Internet Noise (1.1.1.0/24)

Louis Poinsignon

Who am I

Louis Poinsignon

Network Engineer @ Cloudflare.

Working on a network data pipeline.
Decided to dig into the Terabytes of flows.

The IP blocks

Special IP range 1.1.1.0/24 and 1.0.0.0/24.

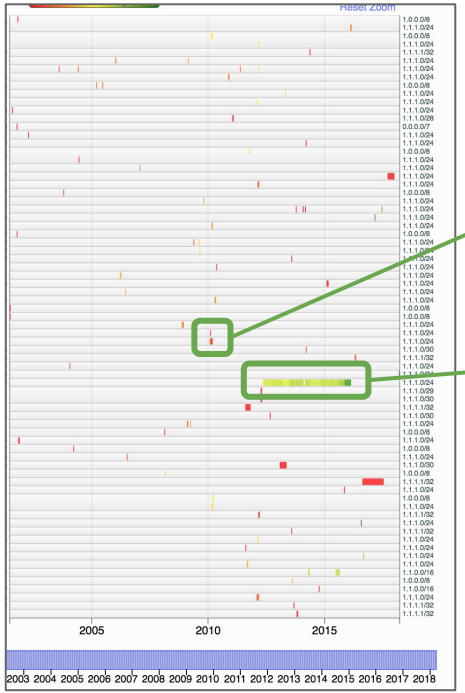
APNIC Labs allowed us to announce it.

Let’s talk about **Internet noise**.

Known to receive unwanted traffic:

- Misconfigurations
- Misuse
  - Proxy
  - Internal use

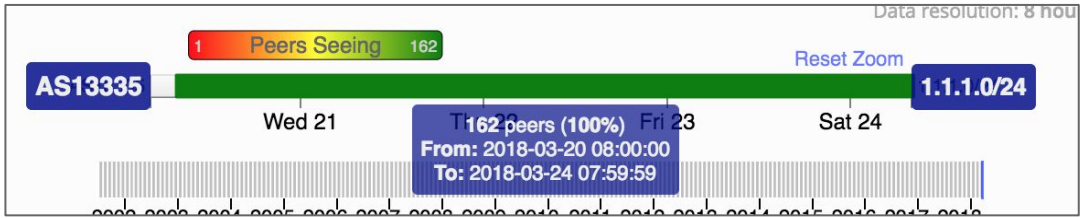
Routing history



RIPE, Merit

```
https://labs.ripe.net/Members/franz/content-pollution-18
- Franz Schwarzinger
http://www.potaroo.net/studies/1slash8/1slash8.html
- Geoff Huston
```

Google, YouTube



CLOUDFLARE

Traffic levels

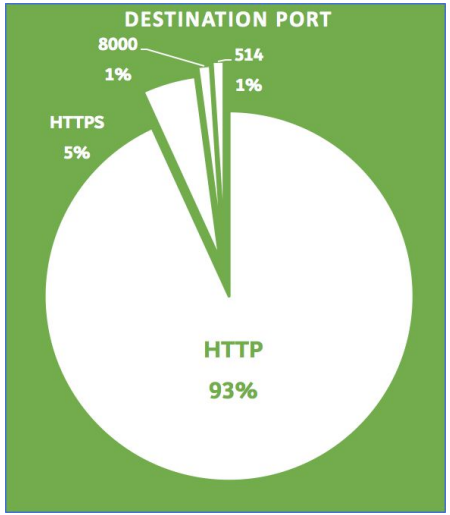
- Previous studies:
  - >100 Mb/s on 1.1.1.0/24 in 2010
  - 100-1Gb/s on 1.0.0.0/8 in 2014
    (https://conference.apnic.net/data/37/2014-02-27-prop-109_1393397866.pdf - Geoff Huston)

- 8-13 Gb/s in 2018
  - 1 Gb/s solely on 1.1.1.1

CLOUDFLARE

Traffic type

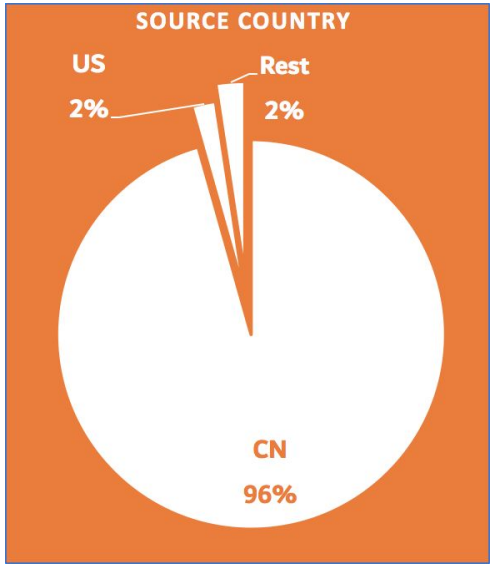
- TCP traffic (mostly HTTP proxy, services).
  - Ports 443, 80, 8000, 8080, 8090, 8765
- UDP traffic (some DNS, syslogs).
  - Ports 53, 514, 8000, 80, 8090
- TP-Link DNS 1.0.0.19
  - https://serverfault.com/questions/365613/tp-link-routers-send-dns-queries-to-1-0-0-19-what-is-that/365630



CLOUDFLARE

Traffic source

Mostly China, US, countries in Asia, some Europe

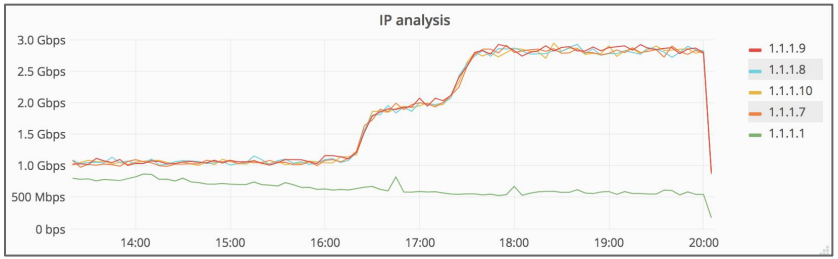


CLOUDFLARE

Bursts and patterns

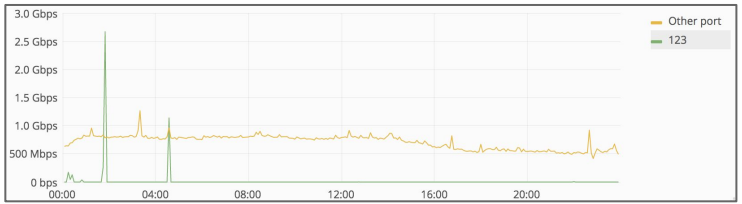
Two increases:

- 5 Gb/s → 8 Gb/s between 1600 and 1715 UTC
- 8 Gb/s → 12.5 Gb/s between 1715 and 2300 UTC
- Mostly on 1.1.1.7, 1.1.1.8, 1.1.1.9 and 1.1.1.10
  - Destination 80
  - Increase from China
  - No particular difference on source IP/net



Short bursts:

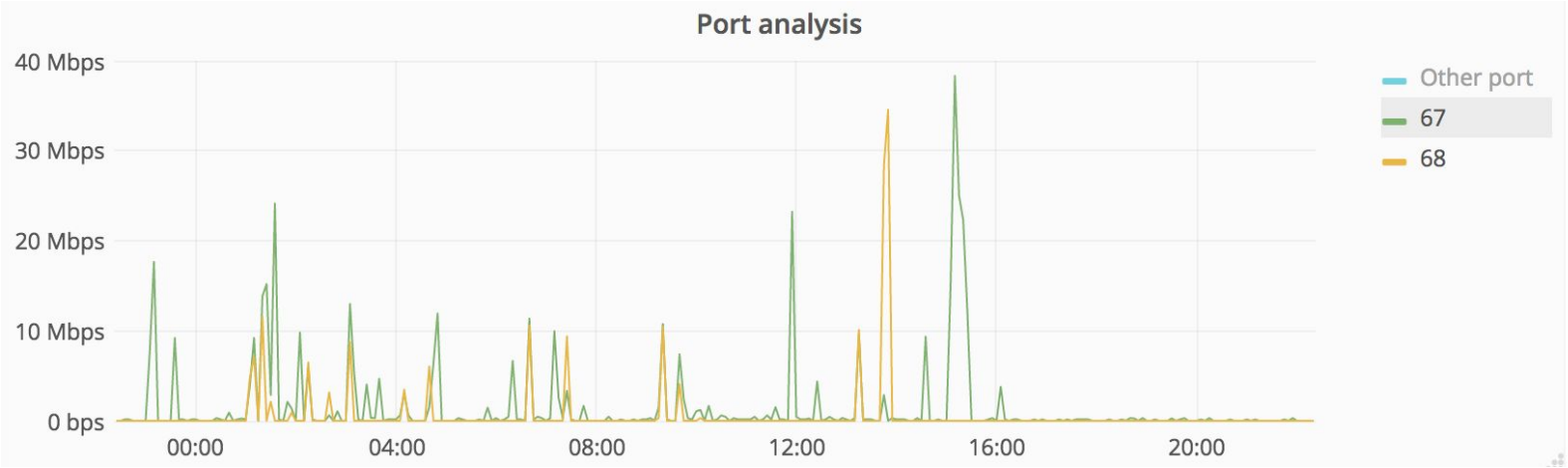
- Only on 1.1.1.1 between 0100 and 0200 UTC for a few minutes
- 1-10 gigabits/sec
- UDP traffic source 123 (NTP) and 11211 (memcached)
  - Misconfigured network devices?



CLOUDFLARE

Bursts and patterns

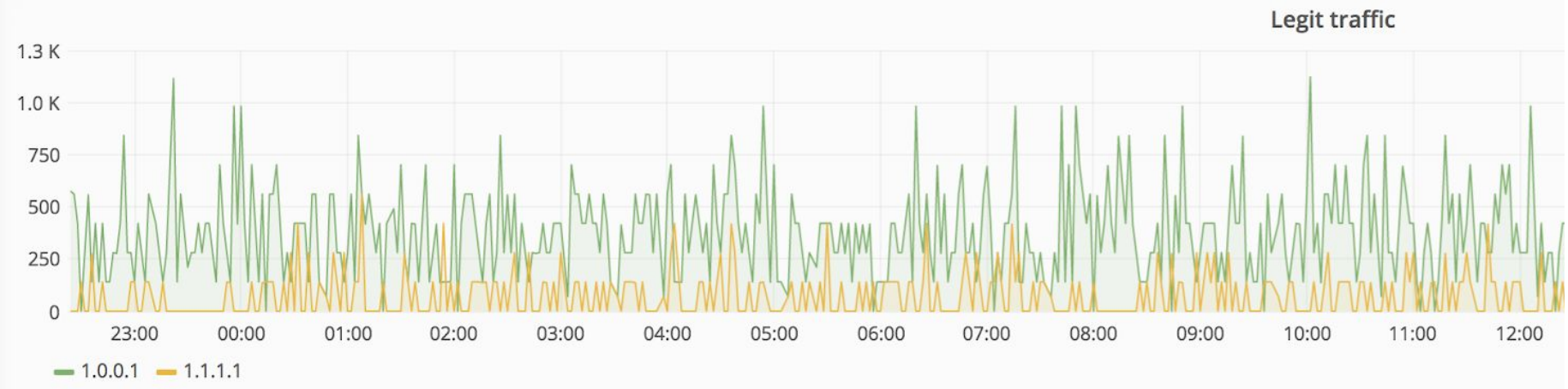
Also DHCP spikes. From **Macau**.



CLOUDFLARE

Almost legit traffic

How many packets per second on UDP 53 (before launching)



CLOUDFLARE

What changed?

Presentation from 10 years ago at NANOG49
(`https://www.nanog.org/meetings/nanog49/presentations/Monday/karir-1slash8.pdf - Merit, APNIC & UMich`)

We still see iperf traffic (port 5000/5001).

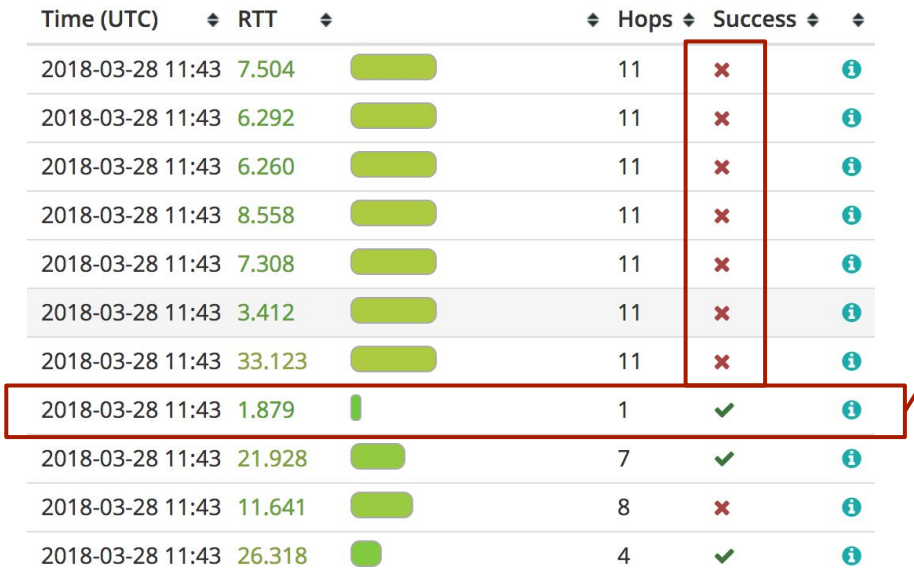
Around **10-20** times the traffic.

We estimate legitimate traffic to be around **7-13%**

CLOUDFLARE

Availability?

Thanks to the Atlas probes, thousands of tests



Time (UTC)	RTT	Hops	Success
2018-03-28 11:43	7.504	11	✗
2018-03-28 11:43	6.292	11	✗
2018-03-28 11:43	6.260	11	✗
2018-03-28 11:43	8.558	11	✗
2018-03-28 11:43	7.308	11	✗
2018-03-28 11:43	3.412	11	✗
2018-03-28 11:43	33.123	11	✗
2018-03-28 11:43	1.879	1	✓
2018-03-28 11:43	21.928	7	✓
2018-03-28 11:43	11.641	8	✗
2018-03-28 11:43	26.318	4	✓

Null-routes

CPE installed in ISP

…

Suddenly an open FTP server

CLOUDFLARE

Availability?

More than **30 major** Internet Service Providers all around the **world** having issues.
Will require a dedicated support queue for issues once the service is announced.

Mostly null-routing 1.1.1.1/32 or ACLs.

But also using 1.0.0.0/24 for internal purposes (finding devices)

Most of the ISPs are cleaning their configurations (more than a dozen fixed in less than a week).
Few non-responses.

Problems

01-13-2017, 03:44 PM #8

Quote:

Getting tired of typing 192.168. Why doesn't everybody use something simple like 1.1.1.x in a small LAN? What about 0.0.0.x?

I have been using 1.1.1.0/24 subnet for 15+ years on my home LAN and have never found a single instance where any computer in my house ever tried connecting to any address inside the 1.1.1.0-255 range outside my house.

Yes, I realize these are 'publically allocated addresses' but I too got very sick and tired of typing 192.168.blah.blah all the time. I do extensive lab stuff for work where I have servers I build and test in my LAN and am constantly typing IPs all the time.

I still have no regrets about using this subnet. In fact, today in my lab work, I also use 1.1.2.0/24, 1.1.3.0/24, 1.1.4.0/24, 1.1.5.0/24, 1.1.6.0/24, 1.1.7.0/24, 1.1.8.0/24, 1.1.9.0/24 and for the 1.1.2. to 1.1.9. range those are only for lab equipment (have no gateways) for things like iSCSI, vMotion, VSAN and stuff like that so I don't care about them anyway.

You know, if everyone in the world started using 1.1.x.x addresses for home and private LAN use then maybe the industry would change their standard and re-allocate these for official private LAN use, since if someone put a web server on those nobody would ever find their way there. They would be unpopular. Or I guess they are already unpopular because I don't see anyone really using them anyway.

TP-Link routers send DNS queries to 1.0.0.19. What is that?

4

I've got a problem with TP-Link soho routers. The DNS forwarder of those routers tends to ignore the DNS servers obtained by DHCP and instead tries sending all DNS requests to this strange IP: 1.0.0.19? That IP doesn't respond.

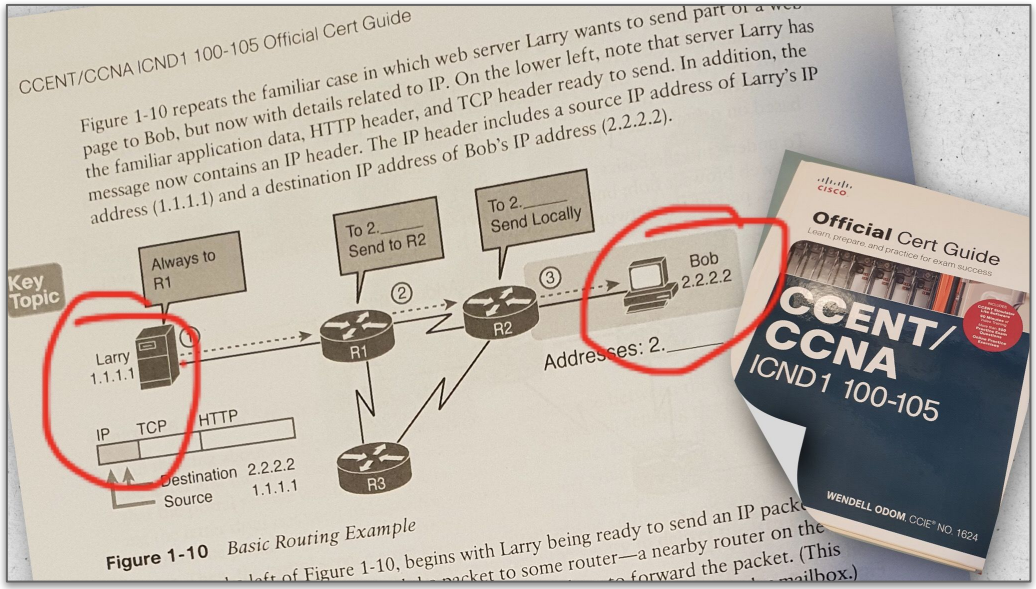
Has anyone else seen that happen?

domain-name-system

CLOUDFLARE

In books

Step 32 In the IP Address text box, enter the IP address of the controller's virtual interface. You should enter a fictitious, unassigned IP address such as 1.1.1.1.



CLOUDFLARE

Conclusions

A lots of providers were not **accepting** the prefix or routing internally.
Trying to **cleanup** and understand the pattern.
Contact some people having **misconfigurations** (sending their syslogs).

The Internet contains a lot of these prefixes that could attract trash traffic.

If enough capacity: leak the prefix, listen to the noise (syslogs, HTTP proxies...).

Questions?

Thank you

louis@cloudflare.com
@lspgn
traceroute6 cv6.poinsignon.org